Task: BentoboxV1 Assesment Audit
Goal: To find vulnerability that can lead to loss of funds
Assigned to: Darshan Jogi
Email: Darshanbughunter@gmail.com

Findings:

1. Inflation Attack in Share Calculation Leads to Loss of Funds

Title: Inflation Attack in Share Calculation Leads to Loss of Funds

Summary

BentoboxV1 smart contract is vulnerable to inflation attack due to share calculation logic issues due to which attackers can take advantage of being first deposited and earn a 1:1 share ratio.

Vulnerability Details
This Smart contract uses **BalanceOf** for accounting and **first depositor** logic which makes smart contract vulnerable to inflation attacks.

Steps To Reproduce Attack-

1. Bob initiates a transaction to deposit 10 ETH into the contract.
2. Alice observes Bob's transaction in the mempool and front-runs it by depositing 1 wei.
   if (total.elastic == 0) { base = elastic; } is true, Alice receives 1 share minted for her 1 wei deposit.
3. Alice sends an additional 10 ETH to the smart contract by calling the receive function.
4. Now Bob's transaction (from Step 1) is processed
   base = elastic.mul(total.base) / total.elastic;
   base = 10 ETH * 1 / (10 ETH + 1 wei)
   base = 0. Bob receives 0 shares minted.
5. Alice withdraws her shares, enabling her to retrieve 20 ETH + 1 wei. Alice is draining the contract.

Impact
Loss of funds

Recommendations
Implement https://docs.openzeppelin.com/contracts/4.x/erc4626